U.S. PIRG

Testimony of the U.S. Public Interest Research Group

Edmund Mierzwinski (ed@pirg.org)
Consumer Program Director

Concerning Affiliate Sharing Practices and the Fair Credit Reporting Act

Before the Senate Banking Committee
Honorable Richard Shelby, Chair

26 June 2003

Chairman Shelby, Senator Sarbanes and members of the committee: On behalf of the non-profit, non-partisan state-based Public Interest Research Groups, U.S. PIRG is pleased to offer you this testimony on affiliate sharing practices and the Fair Credit Reporting Act (FCRA). Among the most important matters before the 108th Congress is review of the impact of the 1996 exception to the definition of credit report allowing companies to share customer experience and transaction information among corporate affiliates outside the major consumer protections of the FCRA.

Our testimony also discusses the relationship between the FCRA and the 1999 Gramm-Leach-Bliley Financial Services Modernization Act (GLB) and attempts by industry to chill efforts by cities and states to enact stronger financial privacy laws, as GLB clearly allows under the Sarbanes states' rights amendment.

In addition to presenting our views on the problems caused by unregulated and under-regulated information sharing by and among corporate affiliates and unaffiliated third parties, we urge the Congress not to extend the FCRA's temporary 1996 partial preemption provisions. The FCRA itself does not need to be reauthorized; extension of preemption is an optional decision by the Congress that, in our view, reverses clear Congressional intent from 1996 that preemption be temporary.

Summary

Congress enacted in 1970 a comprehensive scheme for regulating the sharing of detailed information by credit bureaus under the Fair Credit Reporting Act. Yet, through a 1996 exception, it created a new class of unregulated affiliate sharing transactions. Sharing of confidential consumer information among affiliates is not regulated under the FCRA nor under the Gramm-Leach-Bliley Act. The latter act simply requires notice of affiliate and third party information sharing practices and provides a modest opt-out in an extremely limited subset of third-party transactions. In the post-GLB marketplace, this failure to regulate a growing class of transactions involving confidential consumer information and decision-making is troubling. While we have enacted comprehensive standards for regulating credit reports, we have no standards for regulating affiliate sharing.

Industry, in a series of hearings before this committee and the House Financial Services Committee, has failed to make the case for a continued exception from regulation for affiliate information sharing.

Industry has also claimed, without proof, that unregulated information sharing provides billions of dollars of benefits to the economy and, again without proof, that providing consumers with greater privacy rights will eliminate those alleged benefits. Industry has also claimed that providing consumers with privacy protection will prevent them from stopping fraud or completing transactions on consumer accounts. Neither claim is true. Industry also infers that consumer groups are for "harsh" opt-in rules, but that the pro-consumer industry would support a more reasonable opt-out privacy mechanism. In fact, sharing under the Gramm-Leach-Bliley Act is largely based on a notice only, no-opt regime. The vast majority of the financial services industry prefers no-opt even to modest opt-out protections.

1. The Fair Credit Reporting Act Strictly Regulates Information-Sharing By Credit Bureaus Under The Fair Information Practices, But Allows Companies A Sweeping Affiliate-Sharing Exception to the Definition of Credit Report

A. The Fair Credit Reporting Act, Its History and the Fair Information Practices

I want to state clearly at the outset that the FCRA is an important consumer protection and privacy law. It plays a critical role in helping consumers obtain opportunities in the marketplace. The 1970 Act recognized the importance to the economy of the third-party credit reporting system, but it also recognized the importance of accurate credit reports and the protection of privacy. Yet, despite the 1996 attempts to update the law to improve it, the law still suffers from numerous problems[1] in addition to its affiliate-sharing exception, the subject of today's hearing.

The FCRA was enacted[2] in 1970 in the wake of a series of scandals involving unfair insurance investigations. Congress also recognized an increasing inability of consumers to obtain redress when credit mistakes were made. The 1970 Act created a broad structure for regulating consumer reporting agencies (CRAs, or credit bureaus).

The FCRA's general structure is based on the Code of Fair Information Practices,[3] which were later described by a 1973 Health, Education and Welfare (HEW) task force and embodied into the 1974 Privacy Act,[4] which regulates government uses of information. The Fair Information Practices require data collectors to collect only limited information; to use it only for specified purposes, unless consent of the data subject is granted for secondary uses; to protect the security, accuracy and privacy of that information; to make information practices transparent to subjects; to grant data subjects the rights to inspect, correct and dispute records about them; and, to grant data subjects the right to enforce these rights.

For example, the FCRA allows credit bureaus – which are clearly third parties without a direct relationship with consumers – to obtain detailed information from public records, creditors and even subjective interviews and then to engage in widespread trafficking in detailed credit dossiers containing a consumer's most intimate financial details.

But, the FCRA strictly regulates that trafficking through its comprehensive structure, based on the Fair Information Practices. It requires credit bureaus to employ reasonable procedures to ensure the "maximum possible accuracy" of credit reports. It limits the use of credit reports only to users with a permissible purpose. It gives consumers a series of rights, including a right to inspect the reports (for free after denial of credit) and to dispute errors. It gives consumers a right to learn when their reports have been used adversely, for example to deny them credit or insurance. It gives consumers the right to sue bureaus that make mistakes or refuse to fix them, but it tempers that right with strong affirmative defenses and defamation immunity for the CRAs.

Although the act was not and is not perfect, most experts agree that the FCRA was the first comprehensive privacy law enacted in the U.S. and that its general framework is soundly based on the Fair Information Practices.

In 1989, in response to a series of complaints about credit reporting errors, Congress began a series of hearings that culminated in the 1996 amendments to the FCRA. Three matters of extreme controversy – pitting consumer groups, state attorneys general and, on all major issues

joined by the Federal Trade Commission, against the financial industry – delayed final passage of the amendments from 1992 until 1996.[5]

- First, industry insisted that the FCRA's longstanding floor preemption provision (states can enact stronger laws) be reversed and that the federal FCRA become a ceiling. The final 1996 amendments preempted only some provisions of the FCRA, and then only for 8 years.
- Second, industry fiercely resisted efforts to add a new provision to the act imposing duties on creditors that furnish information to credit bureaus to ensure accuracy and imposing liability when those duties were violated. The final provision imposed only limited duties. Liability for making errors was subjected only to agency enforcement, with consumers only having a private right of action to enforce violations of the act's reinvestigation provisions.
- Third, industry insisted that a new exception to the definition of credit report be carved out, for the sharing of experience and transaction information among companies affiliated by common control. In addition, the new exception was included in the list of provisions subject to the temporary preemption of state action.

B. The Affiliate Sharing Exception to The FCRA

Although numerous hearings were held from 1989-1996 during consideration of the FCRA amendments, we are unaware of any specific hearing on affiliate sharing, nor any record testimony of any significance, if any at all, provided by the industry about the subject. Yet, among state attorneys general, consumer groups and the FTC, there was grave concern that Congress was acting precipitously to create a sweeping exception that could limit consumer access to the wide panoply of rights granted by the FCRA.

The affiliate sharing exception allows detailed experience and transaction information to be shared and used for adverse actions without triggering the FCRA's consumer protection rights,[6] in the circumstance where the information is shared among corporate affiliates. Experience and transaction information could include details from credit card and checking account purchases, mortgage balances and payment histories, bank account and brokerage balances and other deposit account usage information, relationships with co-signers, if any, etc.

As the FTC, in an official position paper,[7] stated on affiliate sharing:

> "Because the subject of information sharing with affiliates has not been the subject of Congressional hearings, the factual basis for the provision is not necessarily available and the Commission cannot easily evaluate its pros-and-cons. The Commission believes, however, that caution is the best approach in considering whether to create what may become a significant exception to the consumer protections provided by the FCRA. It may be preferable to defer creation of any exceptions to the FCRA's protections for affiliate sharing until Congress has an opportunity to study this issue and its implications more carefully."

Congress did not debate affiliate sharing prior to 1996. Prior to enactment of the 1999 Gramm-Leach-Bliley Act, however, Congress finally became acutely aware of the problems posed by unfettered information sharing.

C. The Costs To Consumers of Under-Regulated Affiliate Sharing

In 1999, while it was considering enactment of GLB, a sweeping deregulation of the financial services industry that would encourage the establishment of affiliate-based financial services supermarkets – with banks, brokerages and insurance companies all under one roof -- Congress became aware of the first two in a series of privacy nightmares involving banks and their affiliates.

- First, Nationsbank (now Bank of America) had recently paid civil penalties totaling $7 million to the Securities and Exchange Commission and other agencies, plus millions more in private class action settlements, over its sharing of confidential bank accountholder information with an affiliated securities firm. "Registered representatives also received other NationsBank customer information, such as financial statements and account balances."[8] In this case, conservative investors who held maturing certificates of deposits (CDs) were switched into risky financial derivative products. Some lost large parts of their life savings.
- Second, Minnesota Attorney General Mike Hatch had recently sued US Bank and its holding company, accusing them of having "sold their customers' private, confidential information to MemberWorks, Inc., a telemarketing company, for $4 million dollars plus commissions of 22 percent of net revenue on sales made by MemberWorks."[9] Memberworks and other non-affiliated third party telemarketers sign credit card customers up for add-on "membership club" products and bill their credit cards as much as $89 or more if they do not cancel within 30 days. The catch? The consumer never gave the telemarketer her credit card number; her bank did, in a scheme known as pre-acquired account telemarketing. General Hatch has settled with both US Bank and Memberworks.

While industry continues to claim that these were isolated pre-GLB incidents, many of the nation's largest banks have since been involved in enforcement actions and private litigation over their similar sloppy information practices. Capital One[10], Chase Manhattan[11], Citibank[12], First U.S.A.[13], GE Capital[14], MBNA America[15] are other banks or bank affiliates that have provided their customers' personal and confidential information to fraudulent telemarketers.

While some cynical consumers might expect tawdry marketing behavior from a credit card company, Minnesota Attorney General Mike Hatch also brought an action against a mortgage company, in this case a subsidiary of a national bank. In December 2000, the Minnesota Attorney General filed a complaint against Fleet Mortgage, an affiliate of FleetBoston, for substantially the same types of violations as U.S. Bank had engaged in. Incredibly, the firm was allowing telemarketers to add bills for buying club and roadside assistance plan memberships to consumer mortgage payments after making deceptive telemarketing calls based on confidential information derived from account relationships.[16] That complaint was settled in June 2001.[17] The state's complaint explains the problem with sharing confidential account information with third party telemarketers.

> Other than a cash purchase, providing a signed instrument or a credit card account number is a readily recognizable means for a consumer to signal assent to a telemarketing deal. Pre-acquired account telemarketing removes these short-hand methods for the consumer to control when he or she has agreed to a purchase. The telemarketer with a pre-acquired account turns this process on its head. Fleet not only provides its telemarketing partners with the ability to charge the Fleet customer's mortgage account,

> but Fleet allows the telemarketing partner to decide whether the consumer actually consented. For many consumers, withholding their credit card account number or signature from the telemarketer is their ultimate defense against unwanted charges from telemarketing calls. Fleet's sales practices remove this defense.[18]

Another bank, Charter Pacific, was caught selling its database containing 3.6 million valid credit card account numbers to a convicted felon who then fraudulently billed the accounts for access to Internet pornography sites that victims had never visited.[19] In fact, approximately forty-five percent of the victims did not even own a computer. Charter Pacific did not develop the database from its own customers' information. Instead, it compiled the information from credit card holders who had purchased goods and services from merchants that had accounts at Charter Pacific. The information included the date of sale, account number, and dollar amount of every credit card transaction processed by the bank's merchant customers. The unrestricted sharing of this information resulted in over $44 million of unauthorized charges.

When data collectors do not adhere to Fair Information Practices consumers face numerous privacy risks. A summary of significant privacy costs includes the following:

- Consumers pay a much **higher price** than dinner interruptions from telemarketers. Many unsuspecting consumers may still be paying $89/year or more for essentially worthless membership club products they did not want and did not order. Although the Federal Trade Commission has enacted amendments to the Telemarketing Sales Rule[20] (TSR) in an attempt to regulate the tawdry bank practices described above, additional amendments may be necessary to ensure that banks and their affiliates and subsidiaries comply fully with the amendments, since they may run to the OCC for protection from the FTC otherwise.
- **Easy access** to confidential consumer identifying information leads to identity theft. Identity theft may affect 500-700,000 consumers each year. Identity theft victims in a recent PIRG/Privacy Rights Clearinghouse survey[21] faced average out-of-pocket costs of $808 and average lost time of 175 hours over a period of 1-4 years clearing an average $17,000 of fraudulent credit off their credit reports. It is difficult to measure the costs of higher credit these consumers pay, let alone attempt to quantify the emotional trauma caused by the stigma of having their good names ruined by a thief who was aided and abetted by their bank and credit bureau's sloppy information practices. The committee need only review last week's compelling testimony of Captain John Harrison[22] (Ret.). In his oral statement, in particular, Harrison described how he had gone from a high-achieving military officer to a failed salesman who recently lost his job due to, in his view, his loss of confidence caused by his inability to cope with the frustration and emotional distress of being a victim of identity theft and his subsequent inability to clear his name of 61 fraudulent credit accounts.
- Easy access to **Social Security Numbers** by Internet information brokers and others also leads to stalking.
- The **failure to safeguard** information and maintain its accuracy leads to mistakes in credit reports and consequently consumers pay higher costs for credit or are even denied opportunities.
- Researchers at Michigan State University recently studied over 1000 **identity theft** cases and found that victims in fifty percent of the cases specifically reported that the theft was committed by an employee of a company compiling personal information on individuals.[23] Many identity fraud cases stem from the perpetrator's purchase of consumers' personal

information from commercial data brokers. Financial institutions information sharing practices contribute to the risk of identity theft by greatly expanding the opportunity for thieves to obtain access to sensitive personal information.

- The unlimited collection and sharing of personal data poses **profiling threats**. Profiles can be used to determine the amount one pays for financial services and products obtained from within the "financial supermarket" structure. As just one example, information about health condition or lifestyle can be used to determine interest rates for a credit card or mortgage. Even with a history of spotless credit, an individual, profiled on undisclosed factors, can end up paying too much for a financial service or product. Because there are no limits on the sharing of personal data among corporate affiliates, a customer profile can be developed by a financial affiliate of the company and sold or shared with an affiliate that does not fall within the broad definition of "financial institution." A bank, for instance, that has an affiliation with a travel company could share a customer profile resulting in the bank's customer receiving unwanted telephone calls and unsolicited direct mail for offers of memberships in travel clubs or the like that the individual never wanted or requested. A negative credit decision based on this profile would not trigger the vast consumer protection rights that would be triggered by use of a strictly regulated credit report.[24]
- Further, the lack of any regulation of experience and transaction information may pose risks for the privacy of health data. Confidential medical records held by any health insurer or hospital are strictly regulated by the Health Insurance Portability and Accountability Act (HIPAA)'s medical privacy rules. If that information is obtained by any GLB entity, it could be freely shared outside of HIPAA.[25]

In response to the public uproar over the Nationsbank and U.S. Bank cases, Congress included a privacy title, Title V, in GLB.[26]

2. While the FCRA Is Based On Comprehensive Protections, The Gramm-Leach-Bliley Financial Services Modernization Act's No-Opt Regime Conversely Fails To Adequately Regulate Either Affiliate or Third Party Information Sharing

A. The GLB's No-Opt Regime

Much of the debate over affiliate sharing and financial privacy has not been over whether financial institutions protect information under the Fair Information Practices. Rather, the debate has been over whether banks and other institutions should provide consumers with an express consent right (affirmatively say yes, or opt-in, before sharing) or whether information sharing should be allowed automatically unless the consumer says no (OK to share as long as consumer does not opt-out). Industry documents and materials assert that the debate is over opt-out or opt-in, falsely implying that they are for opt-out, but that opt-in goes too far and would cost too much.

Actually, the vast majority of the financial services industry has yet to agree that even an opt-out is acceptable—most companies are actually for no-opt.

Many observers are unaware that the primary protection Congress established in Gramm-Leach-Bliley is provided only by **notice** (no-opt), **not** by opt-out. The Fair Credit Reporting Act is based broadly on the Fair Information Practices, but GLB is, at best, based on FIPs-Lite. Notice

is not enough. When comprehensive databases of information are held and used by companies, consumers need all of the rights provided by the Fair Information Practices. GLB does not regulate in any way affiliate sharing of experience and transaction. It does not close the loophole established in the FCRA.

Under GLB, sharing of experience and transaction information with either affiliates or with any third party providing joint marketing services is unregulated under a no-opt regime. The rationale for treating marketing partners as affiliates was ostensibly to create a level playing field for smaller institutions that might not have in-house affiliates selling every possible product larger firms might sell. Of course, large firms use joint marketing partners, too.

The limited consumer right to opt-out Congress established only applies in the circumstance where the bank shares experience and transaction information with other third parties selling non-financial services, primarily telemarketers. Even Congressional Research Service reports have misunderstood the modest effect of the limited opt-out provisions of GLB.[27]

GLB should have closed the affiliate sharing exception in the FCRA. It did not. The failure of the GLB to regulate or require any form of consumer consent for the vast majority of information sharing transactions affected is one example of how GLB – unlike the broader FCRA as it applies to credit reports-- fails to meet the Fair Information Practices. GLB fails to adequately protect consumer privacy.

B. Notice is Not Enough

The result of this defective scheme is that most information-sharing is only regulated or "protected" by notice. Sharing of confidential consumer information with either affiliates or joint marketing partners continues regardless of a consumer's privacy preference. Although we have no way of knowing how many joint marketing partners a company may have, we do know how many affiliates some of the largest financial services holding companies and bank holding companies have. For their recent joint comments to the Treasury Department on GLB, state Attorneys General accessed the Federal Financial Institutions Examination Council and Federal Reserve websites and counted affiliates for Citibank (2,761), Key Bank (871) and Bank of America (1,476).[28]

In 2001, a coalition of consumer and privacy groups filed a petition[29] with the agencies responsible for enforcing the GLB Privacy Rule. On an encouraging note, many of the petitioners have recently been informally contacted to watch for agency actions in response to that petition calling for better privacy notices. Some industry members are even supporting improvements to the privacy notices. Of course, improving the notices does not change the flawed GLB approach to the sharing of information among affiliates and third parties.

C. A Comparison of the Regulated and Unregulated Information Sharing of FCRA and GLB

Categories of information regulated by the FCRA and GLB are treated in several different ways. The FCRA strictly regulates consumer credit reports. Credit bureaus sell certain other products, known as credit headers, under an unregulated regime, although recent court decisions have narrowed the credit header exception. Credit bureaus also sell under-regulated pre-screened lists

of consumers derived from credit reports, for credit and insurance related purposes. Pre-screened opt-out notices are hard to find and harder to read; the opt-out mechanism is overly complex and, for a permanent opt-out, a consumer must make a call, receive a notice in the mail, sign it, stamp it and return it.[30]

Information obtained by corporate affiliates, however, is known as either "experience and transaction" information or "other" information and regulated by exception to the FCRA. Title V of GLB provides that once companies have provided customers with notice of their information sharing policies, they can share experience and transaction under the extremely permissive GLB regime, with consumer protection provided primarily by notice only (no-opt).

Information Sharing Under The FCRA and The GLB		
Type of Information	**Shared or Sold By**	**Protection Scheme**
Consumer credit reports and investigative consumer reports	Credit Bureaus	FCRA: Comprehensive regulation under FIPs
Credit headers (Demographic, non-credit related, information derived from credit reports).	Credit bureaus	FCRA: Previously sold under exception to FCRA, but under recent decisions by the DC Circuit, US Court of Appeals, dates of birth[31] and Social Security Numbers[32] can no longer be sold as part of credit headers.
Pre-screened lists of consumers with certain characteristics.[33]	Credit bureaus	FCRA: Moderately regulated, with weak right for consumers to opt-out. Lists cannot be used for general target marketing, only sold for marketing credit or insurance products.
"Experience and Transaction" Information (credit card and checking account purchases, mortgage balances, bank account and brokerage balances and other deposit account usage information, relationships with co-signers, etc.)	Banks, brokerages, insurance companies and other financial institutions	FCRA provides that this information is not regulated as a credit report. GLB: Can be shared with any affiliate or any third party in a joint marketing relationship with bank to sell financial products regardless of customer's privacy preference (No-opt). Customer has right to opt out only if information will be shared with or sold to other third parties, primarily telemarketers.
"Other" Information Obtained from a consumer's application, a consumer's credit report or a consumer's references.	Banks, brokerages, insurance companies and other financial institutions	FCRA: Affiliates can share this information with affiliated companies provided consumer is given a notice and a right to opt-out.
GLB exceptions to opt-out rights	Banks, brokerages, insurance companies and other financial institutions	Under numerous exceptions, opt-outs do not apply to experience and transaction information shared with any affiliate or third party for completion of consumer's transaction, fraud control, government purposes, secondary market underwriting, etc.

C. How The Gramm-Leach-Bliley Act Falls Short of the Fair Information Practices:

First, GLB fails to require any form of consent (either opt-in or opt-out) for most forms of information sharing for secondary purposes, including experience and transaction information shared between and among either affiliates or certain affiliated third parties with "joint marketing agreements." These outside firms are treated as if they were affiliates, under the no-opt regime.

Second, while institutions point out consumers generally have access to and dispute rights over their financial account statements, they have no knowledge of, let alone rights to review or dispute, the development of detailed profiles on them created by financial institutions. California is considering a PIRG-backed proposal to address the problem that consumers have neither knowledge of nor a right to inspect marketing profiles.[34]

Third, while GLB does require disclosure of information practices, numerous reviews of these privacy policies, by outside experts,[35] CALPIRG[36] and others has documented that the policies are unreadable and incomprehensible. None fully explain all uses of information, including the development of consumer profiles for marketing purposes. None list all the affiliates, or even all the types, that they might share information with. None describe the specific products, most of which are of minimal or even negative value to consumers, that third party telemarketers might offer for sale to consumers who fail to opt-out. Yet all the privacy policies make a point of describing how consumers who elect to opt-out will give up "beneficial" opportunities.

Fourth, GLB does not give consumers a private right of action to enforce the law as the FCRA generally does.

D. GLB's Preservation of States' Rights: The Sarbanes Amendment

Congress recognized that GLB did not adequately protect privacy and that Title V was only a modest first step. Indeed, Chairman Shelby pointed this out in his floor remarks in opposition to the bill's enactment in 1999.

> We are about to pass this afternoon a financial modernization bill that represents industry interests in a big way. However, we have forgotten the interests of the most crucial market participant of all in America--the consumer, the American citizen. Under this bill, the consumer has little, if any, ability to protect the transfer of his or her personal nonpublic financial information…I can assure Members these large financial conglomerates will have more information on citizens than the IRS, but we have done virtually nothing to protect the sharing of such nonpublic personal financial information for the American people... First, the opt-out requirement does not apply to affiliate sharing. … Second, the bill includes an exception to the porous opt-out provision that allows two or more financial institutions to share their customers' nonpublic personal information with telemarketers to market financial products or services offered under a so-called joint agreement…I believe these privacy provisions are a sham. I have said it before.[37]

In recognition of the concerns of a bi-partisan group of members, led by Senators Shelby (R-AL) and Sarbanes (D-MD) and Representatives Barton (R-TX) and Markey (D-MA), Congress took the exceedingly rare step of affirmatively and specifically granting the states the right to enact stronger financial privacy laws. In conference committee, the Congress inserted an amendment offered by Senator Sarbanes granting states the right to enact stronger financial privacy laws:

> **Sec. 6807. Relation to State laws**
> (a) In general
> This subchapter and the amendments made by this subchapter shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the

extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this subchapter, and then only to the extent of the inconsistency.
(b) Greater protection under State law
For purposes of this section, a State statute, regulation, order, or interpretation is not inconsistent with the provisions of this subchapter if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under this subchapter and the amendments made by this subchapter, as determined by the Federal Trade Commission, after consultation with the agency or authority with jurisdiction under section 6805(a) of this title of either the person that initiated the complaint or that is the subject of the complaint, on its own motion or upon the petition of any interested party. (Pub. L. 106-102, title V, Sec. 507, Nov. 12, 1999, 113 Stat. 1442.)

The GLB Conference Report illustrates the final statement of the terms agreed to by both houses, which confirms what GLB states explicitly: the states are free to adopt laws regarding the privacy of consumer financial information provided to financial institutions. On the floor, Senator Sarbanes[38] emphasized protection of the states' authority to legislate in the area of consumer privacy:

> [W]e were able to include in the conference report an amendment that I proposed which ensures that the Federal Government will not preempt stronger State financial privacy laws that exist now or may be enacted in the future. As a result, States will be free to enact stronger privacy safeguards if they deem it appropriate.

Likewise, Sen. Grams[39] said the savings clause of GLB "preserves all existing and all future State privacy protections above and beyond the national floor established in this bill." House members similarly interpreted the amended the bill. As Rep. John LaFalce[40] said, "[T]he conference report totally safeguards stronger state consumer protection laws in the privacy area."

3. Industry's Claim That The FCRA's Preemption Provision Trumps GLB's States' Rights Provision Is False, But Its Propaganda Campaign Has Had A Chilling Effect On State Action To Enact Stronger Financial Privacy Laws

The FCRA regulates credit reports. As discussed above, a narrow exception states that when companies share information among corporate affiliates, the sharing does not make the sharing entity a credit bureau, with a credit bureau's concomitant responsibilities and duties. Although that exception is troubling, since it means that companies are able to make credit decisions on the basis of unregulated internal databases, nothing in the legislative history suggests that Congress intended more than that when it exempted affiliate sharing from the FCRA in 1996.

But while the substantial legislative history and the plain language of Section 6807 of the GLB grant states greater rights to enact stronger privacy laws, industry has alleged that a different provision of GLB, Section 6806, renders the Sarbanes amendment meaningless.

A. The Sarbanes Amendment and the FCRA Savings Clause

Section 6806 is the so-called FCRA savings clause and is intended to preserve the **greater** protections of the FCRA strictly regulating credit reports from being weakened by GLB's lesser protections. Industry claims that the FCRA savings clause creates a safe harbor preventing the Sarbanes amendment from applying to affiliate sharing, by allowing the preemptive affiliate sharing exception of FCRA to trump GLB's Sarbanes amendment.

Yet, as former FTC Chairman Pitofsky testified before Congress on financial services modernization, in a 1999 hearing on HR 10, the House bill which became GLB:

> Finally, the bill should make it clear that its privacy provisions do not limit the FCRA's protections to the extent they apply to financial institution files…. If construed to supersede the FCRA, the H.R. 10 privacy provisions would be a major retreat in privacy protections for consumers. Credit reports could be distributed to firms that had no permissible purpose to see them if the consumer did not take the affirmative step of stopping that practice. The Commission believes it essential to eliminate the potential for such an interpretation **by adding a savings clause indicating that, notwithstanding any provisions of H.R. 10, the full protections of the FCRA continue to apply where applicable**.[41] [Emphasis added]

Industry argues that the FCRA savings clause inserted following the FTC Chairman's request instead acts to limit consumer protection. Industry argues that somehow the purpose of the clause is to allow the FCRA's one weaker exception – not its myriad greater protections – to prevail. War is peace. Up is down.

B. State and Local Action Under Sarbanes Amendment

Industry's threats that the Sarbanes amendment is meaningless have had a chilling effect on state efforts to enact stronger financial privacy laws governing affiliate sharing. Although numerous states have considered financial privacy legislation since 1999, only California has come close to enactment of legislation. In California, a compromise version of SB 1, proposed by State Senator Jackie Speier, has passed the State Senate but is currently mired in the Assembly Banking Committee due to industry opposition. The bill would greatly strengthen consumer rights in information sharing. Anticipating that the bill will not pass, consumer groups including CALPIRG and Consumers Union have already collected over 200,000 signatures toward a proposed ballot initiative for March 2004. The ballot initiative is even stronger than SB 1.

Although it remains the consumer group view that the FCRA savings clause of GLB's effect on the Sarbanes amendment should be construed narrowly, it should be noted that the groups planned the ballot referendum for 2004, after the scheduled sunset of FCRA preemption, to clear one additional procedural hurdle: predicted bank litigation.

Indeed, tired of waiting for the state or Congress to act, several California cities and counties led by San Mateo and Daly City, have enacted local financial privacy ordinances modeled after SB 1. The ordinances will take effect on 1 September 2003, but first they must survive court challenges by Bank of America and Wells Fargo, joined by the nation's chief national bank regulator, the Office of the Comptroller of the Currency.[42]

Comparison of Major Consent Features of Financial Privacy Laws and Proposals			
	Sharing With Affiliates	**Sharing With Third Parties With Joint Marketing Agreements**	**Sharing With Unaffiliated Third Parties Selling Non-Financial Products (Telemarketers)**
Gramm-Leach-Bliley	**No-Opt (Notice only)**		**Opt-out**
SB 1 (Speier) and local ordinances in California	**Opt-out**, except certain same-line-of-business affiliates would still be **no-opt.**	**Opt-out**	**Opt-in**
March 2004 Ballot Proposal in California	**Opt-In: All Transactions**		
Note: All laws and proposed bills include exceptions for completing consumer's transaction, fraud control, underwriting, government purposes, etc.			

If the cities lose in court, despite the clear legislative history in their favor, particularly under a National Bank Act preemption argument, it may be appropriate for the Congress to consider a narrow clarifying amendment to GLB that makes it clear that the Sarbanes amendment is the paramount federal rule on financial privacy, **all** other laws notwithstanding.

4. Industry Has Misrepresented The Goal and the Effect Of State Financial Privacy Laws

Throughout the debate over financial privacy and FCRA preemption, industry has engaged in a two-part strategy to confuse the public and decision-makers.

A. First, Industry Claims To Be For Opt-Out, When It Is In Favor Of No-Opt.

As discussed above in the section on GLB, industry muddles the issue of no-opt versus opt-out. For example, a white paper prepared for the industry that is routinely cited by industry witnesses before Congress states the following:

> Congress struck a critical balance in the 1996 FCRA amendments between consumers' interest in reaping the benefits of accessible credit files and their interest in privacy. That balance is reflected in the combination of preemption and opt-out provisions for prescreening and affiliate-sharing. Efforts to fundamentally alter that balance by not reenacting preemption and/or by conditioning prescreening and affiliate-sharing on opt-in threaten to impose considerable costs on consumers, business, and the economy, while not increasing privacy protection.[43]

The paper is wrong on the affiliate sharing opt-out, unless it is cleverly hedging behind the limited "other" information opt-out.[44] It fails to accurately describe the actual no-opt regime in place for affiliate sharing of experience and transaction information. For this and numerous other reasons, one expert observer, an independent privacy consultant, called this paper "shockingly incompetent.[45]"

Industry witnesses refer to a number of other white papers and pseudo-academic documents[46] purporting to prove that either eliminating state preemption or providing greater financial privacy

protections will cost the economy "billions of dollars." In our view, these papers are based on specious assumptions.

- None of the papers measures the costs of not protecting privacy, including the costs of identity theft.
- None of the papers measures the cost to society of inaccurate credit reports caused by mistakes due to lack of enforcement of the federal FCRA.
- None of the papers separates the impact, if any, of the 1996 preemption provisions from other dependent variables or attempts to evaluate the effect of other factors on the credit economy.

None of the industry studies attempt to quantify the costs of not protecting privacy. One contrary study finds, "In fact, the costs incurred by both business and individuals due to incomplete or insufficient privacy protections reach tens of billions of dollars every year."[47]

None of the industry studies measures the costs of inaccurate credit reports. According to just one key finding of a major recent study of 500,000 credit files:

> Misclassification into the subprime mortgage market can require a borrower to overpay by tens of thousands of dollars in interest payments on a typical mortgage. For example, over the life of a 30-year, $150,000 mortgage, a borrower who is incorrectly placed into a 9.84% subprime loan would pay $317,516.53 in interest, compared to $193,450.30 in interest payments if that borrower obtained a 6.56% prime loan – a difference of $124,066.23 in interest payments.

That study, [48] by the Consumer Federation of America and National Credit Reporting Association, found that at least 8 million consumers are at risk of being misclassified into sub-prime credit due to sloppy information handling practices by credit reporting agencies.

None of the industry studies measures the costs of a post-GLB credit economy where adverse decisions are made without consumers gaining the right to know about, look at, dispute or correct their file.

B. Industry Falsely Claims That Financial Privacy Laws Will Stop All Information Sharing, Not Simply Sharing For Secondary Purposes

Perhaps even more importantly, industry's white papers and testimony and press releases have made a wide variety of false and even wild claims about the goal and effect of financial privacy laws:

- Industry alleges that stronger financial privacy laws will prevent firms from using one telephone call center for all of a consumer's accounts.
- Industry claims that financial privacy laws "will hinder their efforts to spot terrorists."[49]
- Industry claims that information sharing is critical to stopping fraud and identity theft.

Actually, the goal of consumer financial privacy laws is not to prevent these uses. SB 1 (California) would simply limit information sharing for secondary purposes without consent. The

goal of SB 27 (California) is to give consumers access rights in GLB that modestly approach those of FCRA.

Here is the anti-fraud, anti-ID theft, exception to the opt-out in existing federal law:

> GLB Section 6802(e) (3)(A) to protect the confidentiality or security of the financial institution's records pertaining to the consumer, the service or product, or the transaction therein; (B) to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; (C) for required institutional risk control, or for resolving customer disputes or inquiries; (D) to persons holding a legal or beneficial interest relating to the consumer; or (E) to persons acting in a fiduciary or representative capacity on behalf of the consumer;

Similar provisions exist for completing a consumer's transaction, underwriting, to comply with government requirements, or to protect the "public safety."

In addition, each of the proposed state and local laws and ballot initiatives, to our knowledge, includes similar exceptions.

It is worse than disingenuous to claim that financial privacy laws, intended to give consumers control over the use of their confidential information for secondary marketing and profiling purposes, will completely close the spigot of information sharing for laudable purposes.

5. Does Information Sharing Prevent Identity Theft? No

Industry has claimed that information sharing is critical to identity theft prevention.

From 1989 through 1996, while Congress considered the strengthening of the FCRA, identity theft was not a significant issue in the debate. While it turns out that the problem was growing, the industry had been keeping it quiet and absorbing the costs of fraud without providing Congress or the FTC with significant information. In 1996, the state PIRGs released the first national report on the problem, "The Consumer X-Files," documenting the cases of several identity theft victims and attempting to quantify the problem.

In 1997, the state PIRGs released a follow-up, "Return To The Consumer X-Files.[50]" In 2000, the state PIRGs and Privacy Rights Clearinghouse released a detailed survey of identity theft victims, "Nowhere To Turn.[51]" In 2003, CALPIRG released the first analysis of police officer views on identity theft, "Policing Privacy[52]." It found that police share consumer groups' views that creditor practices must be reined in to stop identity theft.

In 1998, Congress took its one step to stop identity theft, criminalizing it without reining in the creditor and credit bureau practices that aid and abet the thieves.

The FTC has recently reported that identity theft was the leading complaint to the agency for the years 2000, 2001 and 2002. The number of cases doubled in 2002, according to the FTC. Based on figures reported to the GAO by the credit bureaus themselves, identity theft may strike as many as 500,000-700,000 consumers annually. Criminalization hasn't worked. Do industry's

unbelievable allegations that identity theft is being slowed by information sharing mean the problem would be even worse without information sharing?

Misuse, over-use and easy access to Social Security Numbers is what drives the identity theft epidemic. Fundamentally, this nation needs to wean the private sector of its over-reliance on Social Security Numbers (SSN) as unique identifiers and database keys. Creditors issue credit based on a match between an applicant's SSN and a credit bureau SSN, with no additional verification in many cases that the applicant is actually the consumer whose credit bureau file is accessed. Getting Social Security Numbers out of circulation and improving sloppy credit granting practices, not unfettered information sharing, are the real solutions to the identity theft menace.

6. Changing Industry Practices Limiting Information Sharing, Not The Threat of State Action, Are the Real Threat To The Economy

A. Failure To Report Completely To Game Credit Score Results

This spring, the Federal Reserve Board of Governors released a major study[53] of credit reports. Among its key findings, based on a review of 248,000 credit reports held by one unnamed repository, was the following: fully 70% of consumers had at least one trade line account with incomplete information. The Fed finds this problematic.

> A key measure used in credit evaluation—utilization—could not be correctly calculated for about one-third of the open revolving accounts in the sample because the creditor did not report the credit limit. About 70 percent of the consumers in the sample had a missing credit limit on one or more of their revolving accounts. If a credit limit for a credit account is not reported, credit evaluators must either ignore utilization (at least for accounts without limits) or use a substitute measure such as the highest-balance level. **The authors' evaluation suggests that substituting the highest-balance level for the credit limit generally results in a higher estimate of credit utilization and probably a higher perceived level of credit risk for affected consumers.** [Emphasis added] [54]

Although industry witnesses will testify to a vast "free flow of information" driving our economy that should not be constrained, more and more firms are choosing to stifle the flow of information themselves -- to maintain their current customers as captive customers.

We expect industry witnesses to claim this problem has been resolved. According to the Fed and CFA studies it has not. This month, a major lender told the American Banker newspaper it does not report credit limits: "Capital One has never reported credit limits, for proprietary reasons," Diana Don, a spokeswoman for the McLean, Va., card issuer, said Wednesday. "We feel that it is part of our business strategy and provides competitive advantage."[55]

When a bank intentionally fails to report a consumer's complete credit report information to a credit bureau, that consumer is unable to shop around for the best prices and other sellers are unable to market better prices to that consumer. Even the Comptroller of the Currency, Mr. Hawke, has condemned the practice.[56] So has the FFIEC: "The Agencies are aware that over the last year some financial institutions have stopped reporting certain items of customer credit

information to consumer reporting agencies (credit bureaus). Specifically, certain large credit card issuers are no longer reporting customer credit lines or high credit balances or both.[57]"

B. Affiliate Sharing Regime Provides Fewer Consumer Rights

As we indicated above, the FCRA is an important privacy and consumer protection law. It provides consumers with substantive rights. Yet the growing use of affiliate sharing under GLB for profiling and credit decision-making may lessen the public benefits of the FCRA. If credit decisions are made on the basis of affiliate-shared information, consumers do not have the same bundle of rights as they would under FCRA. As internal creditor databases increase in size and predicative value, either credit decisions or other profiling decisions (whether to even offer a consumer a certain class of product, for example) may more and more be made under the GLB regime. These adverse actions will not result in triggering the same disclosures and rights that consumers obtain under the FCRA. These changes in the marketplace, which are already occurring, mean that consumers may not have the same credit rights in the future. Congress should carefully scrutinize issues related to the lack of consumer rights in the affiliate sharing world, compared to the significant consumer protections provided by the FCRA.

7. Conclusion

Our complex national credit system, which relies on interrelationships between and among furnishers of information (creditors), consumer reporting agencies (credit bureaus) and numerous other information providers, secondary market players and, finally, consumers, was not created by the temporary 1996 preemption compromise to the FCRA and will not be destroyed by letting it expire. Nor was that complex national credit system created by the affiliate sharing regime of GLB which has resulted in a growing number of unregulated transactions and credit decisions.

The FCRA worked well before 1996, as the testimony of the Vermont Attorney General's office and other consumer witnesses has made clear today. Industry's lobbying campaign urging you to simply extend the temporary preemption and extend the non-regulation of affiliate sharing is merely an attempt to preserve the unacceptable status quo that has resulted in unacceptable levels of credit report errors and an epidemic of identity theft. We hope to work with the committee on solutions to these problems as well.

We generally agree with industry that a uniform national law would be the most efficient, provided it is adequate. But the best way to get to **adequate uniformity** is to retain states' rights. Congress has not demonstrated a propensity for enacting uniform consumer protection laws that are adequate, except when driven by the threat of state actions. If Congress fails to solve the problem, or new problems arise, the states can act more quickly to resolve the problem and provide a template for additional federal action by the Congress.

Retaining states' right to enact stronger laws is the best way to guarantee an eventual strong uniform federal law. The states are rational actors; they will not act to balkanize our financial system. Instead, they will respond to new threats with new and innovative ideas, which will be eventually be adopted by other states. The notion of 50 different, conflicting laws is absurd and not even worth debate.

In the area of consumer protection, without ideas from the states, typically the only way the inertia of Congress is ever overcome is by a stark crisis – such as Enron. Remember, the Enron fiasco wasn't even enough to guarantee passage of last year's Sarbanes-Oxley corporate reforms—we had to wait for Worldcom.

We appreciate the opportunity to provide our views on the Fair Credit Reporting Act and affiliate sharing. We look forward to working with you in the future on these and other solutions to the problems consumers face in dealing with creditors, furnishers and identity theft.

---

[1] For example, other problems with the FCRA include a lack of adequate federal agency enforcement, unacceptable limits on private enforcement, an utter disdain for compliance by many creditors when they furnish information to credit bureaus, the failure by the consumer reporting industry to maintain adequate accuracy standards, and the disconnect in the credit granting process that has led to the identity theft epidemic. See U.S. PIRG's testimony before the House Subcommittee on Financial Institutions, 4 June 2003, at http://financialservices.house.gov/media/pdf/060403em.pdf

[2] 15 USC 1681 *et seq.*

[3] Ideally, consumer groups believe that all privacy legislation enacted by either the states or Congress should be based on Fair Information Practices, which were originally proposed by a Health, Education and Welfare (HEW) task force and then embodied into the 1974 Privacy Act and into the 1980 Organization for Economic Cooperation and Development (OECD) guidelines. The 1974 Privacy Act applies to government uses of information. Consumer and privacy groups generally view the following as among the key elements of Fair Information Practices: **1) Collection Limitation Principle:** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. **2) Data Quality Principle:** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date. **3) Purpose Specification Principle:** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. **4) Use Limitation Principle:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except: a) with the consent of the data subject; or b) by the authority of law. **5) Security Safeguards Principle:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data. **6) Openness Principle:** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller. **7) Individual Participation Principle:** An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended. **8) Accountability Principle:** A data controller should be accountable for complying with measures which give effect to the principles stated above.
This analysis derived from Robert Gellman, "Privacy, Consumers, and Costs: How The Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete," March 2002, http://www.epic.org/reports/dmfprivacy.html or http://www.cdt.org/publications/dmfprivacy.pdf which also discusses in detail the OECD *Council Recommendations Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 20 I.L.M. 422 (1981), O.E.C.D. Doc. C (80) 58 (Final) (Oct. 1, 1980), at <http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM>

[4] 5 USC 552a

[5] In the interim, a number of states, including Vermont (1992), California (1994) and Masschusetts (1995) acted more quickly to address credit reporting problems.

[6] The 1996 amendments do provide that consumers be provided an extremely limited notice if affiliate shared information is used adversely, but provision of the notice triggers no additional rights. See FCRA Section 615(b)(2). Compare with notice under 615(a) (adverse action based on credit report), which triggers comprehensive rights and duties under Sections 609, 610, 611.

[7] The FTC took an official position on the proposed FCRA amendments in 1994. U.S. PIRG has archived a (scanned) copy of the document, "HR 1015, Federal Trade Commission Analysis and Recommendations, 25 July 1994," at http://www.pirg.org/consumer/credit/ftcanalysishr1015.pdf
[8] See the SEC's Nationbank Consent Order <http://www.sec.gov/litigation/admin/337532.txt>
[9] See the complaint filed by the State of Minnesota against US Bank <http://www.ag.state.mn.us/consumer/privacy/pr/pr%5Fusbank%5F06091999.html>
[10] Office of the Washington State Attorney General, "Settlement with Discount Buying Club Highlights Privacy Concerns," Aug. 4, 2000, http://www.wa.gov/ago/releases/rel_branddirect_080400.html.
[11] *Id.*
[12] National Association of Attorneys Generals, "Multistate Actions: 27 States and Puerto Rico Settle with Citibank," Feb. 27, 2002, http://www.naag.org/issues/20020301-multi-citibank.php; Settlement document available at http://www.oag.state.ny.us/press/2002/feb/feb27b_02_attach.pdf .
[13] Office of the New York Attorney General, "First USA to Halt Vendor's Deceptive Solicitations," Dec. 31, 2002, http://www.oag.state.ny.us/press/2002/dec/dec31a_02.html.
[14] *Supra*, note 1.
[15] *Id.*
[16] See testimony of Minnesota Attorney Mike Hatch before this committee, 19 September 2002 at http://banking.senate.gov/02_09hrg/091902/index.htm
[17] *Minnesota v. Fleet Mortgage Corp.*, 158 F. Supp. 2d 962 (D. Minn. 2001), *available at* http://www.ag.state.mn.us/consumer/PR/Fleet_Opinion_61901.html.
[18] 28 December 2000, Complaint of State of Minnesota vs. Fleet Mortgage, see <http://www.ag.state.mn.us/consumer/news/pr/Comp_Fleet_122800.html>
[19] Federal Trade Commission, "FTC Wins $37.5 Million Judgment from X-Rate Website Operator; Bank Sold Defendants Access to Active MasterCard, Visa Card Numbers," Sept. 7, 2000, http://www.ftc.gov/opa/2000/09/netfill.htm.
[20] The amendments took effect 31 March 2003. http://www.ftc.gov/opa/2003/01/tsrfrnfinal.htm
[21] See "Nowhere To Turn: A Survey of Identity Theft Victims, May 2000,CALPIRG and Privacy Rights Clearinghouse, <http://calpirg.org/CA.asp?id2=3683&id3=CA&>
[22] Senate Banking Committee Hearing On Identity Theft, 19 June 2003. See Captain Harrison's testimony at http://banking.senate.gov/03_06hrg/061903/harrison.pdf.
[23] Personal communication from author to Chris Hoofnagle of EPIC. Study forthcoming; results provided in email from Judith M. Collins, Ph.D., Associate Professor, Leadership and Management Program in Security School of Criminal Justice, Michigan State University to EPIC (Apr. 22, 2003, 18:13:35 EST) (on file with EPIC).
[24] For additional discussion of the profiling issue, and related privacy threats posed by information sharing, see 1 May 2002 comments of EPIC, US PIRG, Consumers Union, and Privacy Rights Clearinghouse on the GLBA Information Sharing Study (Federal Register: February 15, 2002 (Volume 67, Number 32)) available at <http://www.epic.org/privacy/financial/glb_comments.pdf>
[25] See testimony on medical privacy of Joy Pritts, Georgetown University and Marc Rotenberg, EPIC, House Financial Institutions Subcommittee, 7 June 2003 at http://financialservices.house.gov/hearings.asp?formmode=detail&hearing=231
[26] 15 U.S.C. §§ 6801-09
[27] See for example, "Financial Privacy -- The Economics of Opt-In vs Opt-out. (Updated 16 Apr 2003) by CRS's Loretta Nott. It repeats a mischaracterization of GLB that I believe has been made in other CRS reports. The third sentence states: "A consumer's financial information may be shared among the (affiliates of the same corporate) group as long as the person has been notified and has the opportunity to decline, or "opt-out." The paragraph goes on to wrongly say that the Johnson S 660/Tiberi HR 1766 proposals are intended, among other things, to "maintain the opt-out policy for affiliate information sharing."
[28] See 1 May 2002 Attorneys General Comments http://www.ots.treas.gov/docs/r.cfm?95421.pdf or <http://www.epic.org/privacy/financial/ag_glb_comments.html> on the GLBA Information Sharing Study (Federal Register: February 15, 2002 (Volume 67, Number 32))
[29] The petition is available at http://www.privacyrightsnow.com/glbpetition.pdf . See the website http://www.privacyrightsnow.com for additional information about the coalition.
[30] See PIRG's testimony before the House Financial Institutions Subcommittee, 4 June 2003 for a detailed analysis. http://financialservices.house.gov/media/pdf/060403em.pdf

[31] The DC Circuit's 2001 decision is F. 3d 809 (2001). http://laws.findlaw.com/dc/001141a.html The Supreme Court also denied cert (536 US ___(2002) 01-1080, 10 June 2002) in *Trans Union I vs. FTC*, which ended ten years of litigation over Trans Union's illegal use of credit reports for target marketing.
[32] Trans Union II vs. FTC, See http://laws.findlaw.com/dc/015202a.html This important appellate decision upheld the constitutionality of the GLB privacy regulations and restricted the sale of non-public personal information, including Social Security Numbers, by credit bureaus outside of the strict FCRA regime.
[33] The pre-screening opt-out doesn't stop the flow of credit card solicitations, it only slows it down. Now, many retailers, airlines, organizations and others routinely send credit card solicitations to their customers. Yet, these offers are based on affiliate sharing -- under the Gramm-Leach-Bliley Act, not the FCRA. No credit report was used for pre-screening, so no opt-out is provided on the mailings. Under Gramm-Leach-Bliley, affiliate sharing of "experience and transaction" information is subject to a no-opt rule. The FCRA opt-out does not apply, nor does the limited GLB opt out. Congress should create a "no credit card offers" list and apply the 1-call opt-out to all credit card solicitations not only pre-screened solicitations.
[34] Proposed California legislation, SB 27, offered by State Senator Liz Figueroa, would require a business that discloses a consumer's personal information to a third party for direct marketing purposes to provide to a customer, upon request, a written description of the sources and recipients of that information and copies of the information disclosed. See
http://www.leginfo.ca.gov/pub/bill/sen/sb_0001-0050/sb_27_cfa_20030507_132723_sen_comm.html
[35] Mark Hochhauser, readability consultant to the Privacy Rights Clearinghouse, analyzed dozens of the initial notices: "Readability analyses of 60 financial privacy notices found that they are written at a 3rd-4th year college reading level, instead of the junior high school level that is recommended for materials written for the general public. See "Lost in the Fine Print: Readability of Financial Privacy Notices" by Mark Hochhauser at http://www.privacyrights.org/ar/GLB-Reading.htm.
[36] See the CALPIRG report Privacy Denied: A Survey Of Bank Privacy Policies, 15 Aug 2002, <http://calpirg.org/CA.asp?id2=7606&id3=CA&>
[37] 145 CR S13895 Floor remarks of Senator Richard Shelby (R-AL), 4 Nov 1999, during consideration of S. 900, which became GLB.
[38] 145 Cong. Rec. S13789 (1999) Statement of Sen. Sarbanes on final passage of GLB.
[39] 145 Cong. Rec. S13889 (1999) Statement of Sen. Grams.
[40] 145 Cong. Rec. E 2310 (1999) Statement of Rep. LaFalce.
[41] Testimony of FTC Chairman Robert Pitofsky before the House Financial Institutions Subcommittee on HR 10, 21 July 1999, at http://financialservices.house.gov/banking/72199pif.htm
[42] For more information about OCC's abusive preemption positions generally, see http://www.pirg.org/occwatch.
[43] Financial Privacy, Consumer Prosperity, and The Public Good: Maintaining The Balance.
Fred Cate, Robert E. Litan, Michael Staten, Peter Wallison.. Mar 2003. See
http://www.aei.brookings.org/publications/abstract.php?pid=313
[44] See FCRA, Section 604 (d)(2)(A)(iii) concerning information obtained from "other" sources, sucha s a consumer's credit report or application or references.
[45] "No Fair Fight Over FCRA Provision," by Robert Gellman, DM News, 6 May 2003.
[46] Harvard Law School Professor Elizabeth Warren, co-author of several major peer-reviewed studies of the impact of bankruptcy on consumers, has written an extensive article criticizing the use of "proprietary" research (data not available or peer-reviewed, paid for by industry associations that hire academic "research" centers) to make public policy. Wisconsin Law Review Vol. 2002, No. 1, "The Market For Data: The Changing Role of Social Sciences in Shaping The Law," Public Law Research Paper No. 038 See
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=332162
[47] "Privacy, Consumers, and Costs: How The Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete," by Robert Gellman, March 2002, See
http://www.epic.org/reports/dmfprivacy.html See
[48] "Credit Score Accuracy and Implications for Consumers", December 17, 2002, Consumer Federation of America and the National Credit Reporting Association
http://www.consumerfed.org/121702CFA_NCRA_Credit_Score_Report_Final.pdf
[49] "Privacy Laws Under Attack," Associated Press, 19 Feb 2002. The article quotes executives of two powerful industry associations opposing state privacy laws on terrorism grounds: The Financial Services Roundtable (We would have trouble communicating with law enforcement…")and the Financial Services Coordinating Council (""I don't think that explicitly a legislator would try to hurt the exchange of information that would allow law enforcement to do what they need to do…")

[50] See http://www.pirg.org/reports/consumer/xfiles/index.htm
[51] See http://calpirg.org/CA.asp?id2=3683&id3=CA&
[52] See http://www.pirg.org/alerts/route.asp?id2=9791
[53] See "An Overview of Consumer Data and Credit Reporting," Avery et al, February 2003, Pages 47-73, Federal Reserve Bulletin http://www.federalreserve.gov/pubs/bulletin/2003/0203lead.pdf
[54] See page 71, "An Overview of Consumer Data and Credit Reporting," Avery et al, February 2003, Pages 47-73, Federal Reserve Bulletin http://www.federalreserve.gov/pubs/bulletin/2003/0203lead.pdf
[55] "FCRA Hearing to Shine Spotlight on Credit Process," American Banker, 12 June 12, 2003 by Michele Heller
[56] See speech by Comptroller of the Currency John Hawke at http://www.occ.treas.gov/ftp/release/99-51.txt
7 June 1999: "Some lenders appear to have stopped reporting information about subprime borrowers to protect against their best customers being picked off by competitors. Many of those borrowers were lured into high-rate loans as a way to repair credit histories." According to U.S. PIRG's sources in the lending industry, this practice continues.
[57] See advisory letter of18 January 2000 at http://www.ffiec.gov/press/pr011800a.htm